UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/727,953	11/30/2000	Guy McIlroy	PALM-3281.US.P	5875

49637 7590 02/04/2011

BERRY & ASSOCIATES P.C.
9229 SUNSET BOULEVARD
SUITE 630
LOS ANGELES, CA 90069

EXAMINER	
KHOSHNOODI, NADIA	
ART UNIT	PAPER NUMBER
2437	

MAIL DATE	DELIVERY MODE
02/04/2011	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/727,953	MCILROY, GUY	
	Examiner	Art Unit	
	NADIA KHOSHNOODI	2437	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communcation, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 November 2010*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1 and 4-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1, 4-21* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *17 May 2007* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

Claims 2-3 and 22-28 have been cancelled. Applicant's arguments/amendments with respect to the pending claims filed 11/30/2010 have been fully considered but are not persuasive. The Examiner would like to point out that this action is made final (See MPEP 706.07a).

Response to Arguments

Applicants contend that "neither citation references a pre-synchronization scan, a validator program, an emulator, or scanning software by the validator program in a secure environment." Applicants also contend "Wentker contains no concept of a pre-synchronization scan…" and that the cited "passage does not state that the software is marked with a flag during any validation process that would possible deny the software the ability to run on the system and deny synchronization." Examiner respectfully disagrees. A synchronization phase is merely a phase where the software in one device may be transferred to another so that both have the same information. Therefore, pre-synchronization (as used in the scope of the claim) would be any phase before the synchronization/loading phase occurs. Furthermore, Applicants only specify that the software is loaded on the open platform system and does not specify which element of the open platform system comprising of a host facility and portable computing device (as well as possible other nodes within the system) actually loads the software in a manner that initiates a pre-synchronization scan. Wentker et al. teach, prior to loading the software from a smart card to a host device, a pre-synchronization scan to ensure that the application approved by the card issuer is identical to that received by the card manager (col. 12, lines 49-57). Furthermore,

Wentker et al. teach several other portions where scans occur prior to the phase where the software is eventually loaded onto the host device (col. 15, lines 6-15). Specifically, Wentker et al. teach that the software may be checked for viruses and other threats (col. 15, lines 14-15). It is clear from the previous citation that Wentker et al. teach utilization of some type of validation program running within the system (again, within any element of the open platform system since the claims fail to specify) in order to check for potentially harmful behavior within each application. Wentker et al. further teach that based on the result of the pre-synchronization scan and running the validator program, the application may be marked as being "certified" if it behaves properly and is thus cleared to be loaded (col. 15, lines 15-19), i.e. marking the software as valid (where it is obvious/well-known that it would contrarily be considered invalid and not cleared for loading if it is not marked as "certified"). Once the application is certified, only then is it cleared for loading, and in that instance there are still several more authentication steps that may also take place prior to the synchronization phase (col. 17, lines 4-15). The card-locking feature mentioned in col. 9, lines 34-65 plays a role in all of this since it explicitly states that the "card manager 104 can take control of the application life cycle if the card or the issuer **detects a security problem** or if the application is to be deleted" (col. 9, lines 63-65). The previous portion of Wentker et al. suggests that the software may automatically be denied the ability to operate/be synchronized within the open platform system if a security problem has been detected and the application fails to operate in a secure manner. Applicant also state, "there would be no conceivable reason for a third party to test a piece of software only to mark the software as unusable and still enable it to be distributed to the issuer for use on a smart card." Examiner would like to point out that the system of Wentker et al. comprises several phases when an

application is developed, where the first phase is testing the software, another step is authenticating the source/integrity, and a final stage is synchronization. Therefore, testing a piece of software within the open platform system disclosed in Wentker et al. allows for a step of ensuring that the application behaves appropriately, and if it does marking it as "certified" (col. 15, lines 15-19). On the contrary, if it is determined that it is not behaving as it should, it is denied from entering future phases until it has been fixed to perform properly (col. 9, lines 63-65). Therefore, it is not the case where software is tested, marked as unusable, and still distributed in the unusable form to future stages of the process disclosed in Wentker et al. Examiner would also like to note that the claimed limitations do not limit the Examiner from interpreting the pre-synchronization phase as the application testing phase since it occurs before synchronization within the open platform system. Furthermore, the claims do not limit the scope of the invention to a state where another validation check/scan is implemented after the software industry has already done their check and directly before loading the software onto the host. Again Examiner would like to emphasize that the "pre-synchronization scan" as claimed does not state an exact order of where the pre-synchronization scan occurs within the system, it only indicates that it occurs before the synchronization phase.

Applicants mention in their arguments that the functionality described in Wentker et al. "is in no way connected to a validation program that employed an emulator to detect malicious code right before synchronization." In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., "**right before** synchronization") are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read

into the claims. See In re Van Geuns, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). The claims merely state that a pre-synchronization scan occurs but do not limit the pre-synchronization scan to occurring directly prior to the synchronization/loading process. Instead, Applicants claims call for validating software during a pre-synchronization scan within the open platform computer system. Wentker et al. teach an open platform system as the environment for the invention disclosed (col. 20, lines 15-22), where several scans occur prior to the phase where the software is eventually loaded onto the host device (col. 15, lines 6-15). Specifically, Wentker et al. teach that the software may be checked for viruses and other threats (col. 20, lines 14-15).

Furthermore, Applicants contend "at no time is the software to be loaded scanned or validated during a pre-synchronization scan by an emulator" and that "there is no mention of running an emulator in a modified operating system so that the code may be examined for malicious routines as claimed." Examiner respectfully disagrees. Wentker et al. teach a pre-synchronization phase which implements a validator program in order to determine if a particular application contains viruses or other security threats (col. 15, lines 6-15). Muttik et al. was introduced since Wentker et al. failed to explicitly disclose wherein the act of scanning and validating comprises running the code in an emulator for the open platform computer system within the secure environment comprising a modified operating system for the emulator to run in, allowing the execution of the code to be examined for any new malicious routines as well as against known malicious signatures. However Muttik et al. teach using an emulator to run code in order to analyze the code to determine if any malicious routines or known malicious signatures are found (col. 4, lines 4-23). One of ordinary skill in the art would have been

motivated to run the application (which is potentially harmful) in an emulator in a modified operating system since Muttik et al. suggest (and it was well known in the art at the time the invention was made) that emulating the code in a protected region first prevents the code from damaging a computer system in col. 4, lines 15-23. Furthermore, in response to Applicant's argument that there is no teaching, suggestion, or motivation to combine the references, the examiner recognizes that obviousness may be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See In re Fine, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988), In re Jones, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992), and KSR International Co. v. Teleflex, Inc., 550 U.S. 398, 82 USPQ2d 1385 (2007). In this case, Muttik et al. specifically state "Emulator buffer 201 and emulator code 203 are designed so that while suspect code 108 that is executing within emulator buffer 201, s**uspect code 108 cannot damage or compromise computer system** 106" (col. 4, lines 18-22).

Finally, Applicants contend that "Muttik's scope does not include and thus does not disclose 'a computer system comprising a host facility and a portable computer device coupled to the host facility' (emphasis added)." Examiner would like to point out that Muttik was not relied upon for this feature. Wentker et al. teach the open platform computer system comprising the host facility and the portable computing device (col. 4, lines 43-63 and col. 12, lines 9-21). In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See In re Keller, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); In re

Merck & Co., 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986). In this case, the combination of Wentker et al. and Muttik et al. teach/suggest the claimed invention, including the limitation that states the open platform computer system comprises a host facility and portable computing device.

Due to the reasons stated above, the Examiner maintains rejections with respect to the pending claims. The prior arts of records taken singly and/or in combination teach the limitations that the Applicant suggests distinguish from the prior art. Therefore, it is the Examiner's conclusion that the pending claims are not patentably distinct or non-obvious over the prior art of record as presented.

Claim Rejections - 35 USC § 103

I. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

II. Claims 1, 4-5, 8-13, 15-18, and 20-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wentker et al., US Patent No. 6,481,632 and further in view of Muttik et al., US Patent No. 6,907,396.

As per claim 1:

Wentker et al. substantially teach a method of ensuring the security of an open platform computer system, comprising loading software suitable for operating on an open platform computer system in a secure environment on the open platform computer system comprising the

host facility and the portable computing device (col. 4, lines 43-63 and col. 12, lines 9-21); upon loading the software on the open platform computer system, initiating a pre-synchronization scan (col. 12, lines 49-57); during a pre-synchronization scan, validating the software by the use of a validator program residing in the open platform computer system in a secure fashion such that the validator program scans the software that is loaded in a secure environment (col. 15, lines 8-19); marking the software as valid or invalid by the use of a flag (col. 15, lines 15-19); and, automatically denying the software the ability to operate on any environment within the computer system and denying synchronization of the software with the portable computer device if the validator fails to identify the software as valid in order to ensure the security of the open platform computer system (col. 9, lines 34-65 and col. 10, lines 31-39).

Not explicitly disclosed is wherein the act of scanning and validating comprises running the code in an emulator for the open platform computer system within the secure environment comprising a modified operating system for the emulator to run in, allowing the execution of the code to be examined for any new malicious routines as well as against known malicious signatures. However Muttik et al. teach using an emulator to run code in order to analyze the code to determine if any malicious routines or known malicious signatures are found (col. 4, lines 4-23). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Wentker et al. to scan the software in an emulator to discover any malicious routines or known malicious signatures that may be present in the code. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Muttik et al.

suggest that emulating the code in a protected region first prevents the code from damaging a computer system in col. 4, lines 15-23.

As per claim 4:

Wentker et al. and Muttik et al. substantially teach the method described in claim 1. Furthermore, Wentker et al. teach wherein said software is supplied by a third-party source (col. 13, lines 40-60).

As per claim 5:

Wentker et al. and Muttik et al. substantially teach the method described in claim 4. Furthermore, Wentker et al. teach wherein said third-party software is for execution or other use on a palmtop computer (col. 4, lines 43-63).

As per claim 8:

Wentker et al. substantially teach a method of ensuring the security of an open platform computer system, comprising a validations program residing on the open platform computer system in a secure fashion that is configured for: a portable computing device coupled to a host computer, wherein the portable computing device is configured to load software from the host computer to the portable computing device for operating on the portable computing device (col. 12, lines 9-21); a validation program residing on the open platform computer system in a secure fashion (col. 12, lines 49-57) that is configured for: validating the software during a pre-synchronization scan by first scanning the software that is loaded in a secure environment (col. 15, lines 8-19); marking the software as valid or invalid by the use of a flag (col. 15, lines 15-19); and, automatically denying the software the ability to operate on any environment within the computer system and denying synchronization of the software with the portable computing

device if the validator fails to identify the software as valid in order to ensure the security of said computer system (col. 9, lines 34-65 and col. 10, lines 31-39).

Not explicitly disclosed is wherein the act of scanning and validating comprises running the code in an emulator for the open platform computer system within the secure environment comprising a modified operating system for the emulator to run in, allowing the execution of the code to be examined for any new malicious routines as well as against known malicious signatures. However Muttik et al. teach using an emulator to run code in order to analyze the code to determine if any malicious routines or known malicious signatures are found (col. 4, lines 4-23). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Wentker et al. to scan the software in an emulator to discover any malicious routines or known malicious signatures that may be present in the code. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Muttik et al. suggest that emulating the code in a protected region first prevents the code from damaging a computer system in col. 4, lines 15-23.

As per claim 9:

Wentker et al. and Muttik et al. substantially teach the apparatus described in claim 8. Furthermore, Muttik et al. teach wherein said host computer is coupled to a network (col. 3, lines 54-62).

As per claim 10:

Wentker et al. and Muttik et al. substantially teach the apparatus described in claim 8. Furthermore, Wentker et al. teach wherein the portable computing device is a handheld

computing device (col. 4, lines 43-63).

As per claim 11:

Wentker et al. and Muttik et al. substantially teach the apparatus described in claim 8. Furthermore, Wentker et al. teach wherein the portable computing device is a personal data assistant (col. 4, lines 43-63).

As per claim 12:

Wentker et al. and Muttik et al. substantially teach the apparatus described in claim 8. Furthermore, Wentker et al. teach wherein the portable computing device is coupled to said host computer by an infrared device (col. 5, lines 28-40).

As per claim 13:

Wentker et al. and Muttik et al. substantially teach the apparatus described in claim 8. Furthermore, Wentker et al. teach wherein the portable computing device is coupled to said host computer by an RF enabled device (col. 5, lines 28-40).

As per claim 15:

Wentker et al. and Muttik et al. substantially teach the apparatus described in claim 8. Wentker et al. further teach wherein said validation program is configured to evaluate third-party software and attach a digital "valid" flag if the third-party software is found to be clean of known security compromising routines or attach a digital "invalid" flag to the third-party software if the third-party software is not found to be clean of known security compromising routines (col. 12, line 58 – col. 13, line 10 and col. 15, lines 1-19).

As per claim 16:

Wentker et al. and Muttik et al. substantially teach the apparatus described in claim 15. Wentker et al. further teach wherein said portable computing device is configured to load third-party software files with the digital "valid" flag attached and to refrain from loading third-party software files which have no flag attached or have the "invalid" flag attached (col. 15, lines 1-51).

As per claim 17:

Wentker et al. and Muttik et al. substantially teach the apparatus described claim 15. Furthermore, Wentker et al. teach wherein said portable computing device is a personal data assistant (col. 4, lines 43-63).

As per claim 18:

Wentker et al. substantially teach an apparatus of ensuring the security of an open platform computer system, comprising a validations program residing on the network that is configured for: a handheld computing device coupled to a network, wherein the handheld computing device is configured to load software from the network to the handheld computing device for operation on the handheld computing device (col. 4, lines 43-63 and col. 12, lines 9-21); validating the software by scanning files of the software in a secure environment on the handheld computing device upon loading the software in any environment on the handheld computing device (col. 12, lines 49-57); marking the software as valid or invalid by the use of a flag (col. 15, lines 15-19); and, automatically denying the software the ability to operate on any environment within the computer system if the validator fails to identify the software as valid in order to ensure the security of said computer system (col. 9, lines 34-65 and col. 10, lines 31-39).

Not explicitly disclosed is wherein the act of scanning and validating comprises running the code in an emulator for the open platform computer system within the secure environment comprising a modified operating system for the emulator to run in, allowing the execution of the code to be examined for any new malicious routines as well as against known malicious signatures. However Muttik et al. teach using an emulator to run code in order to analyze the code to determine if any malicious routines or known malicious signatures are found (col. 4, lines 4-23). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Wentker et al. to scan the software in an emulator to discover any malicious routines or known malicious signatures that may be present in the code. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Muttik et al. suggest that emulating the code in a protected region first prevents the code from damaging a computer system in col. 4, lines 15-23.

As per claim 20:

Wentker et al. and Muttik et al. substantially teach the apparatus described in claim 18. Wentker et al. further teach wherein said portable computing device is configured to load third-party software files with the digital "valid" flag attached and to refrain from loading third-party software files which have no flag attached or have the "invalid" flag attached (col. 15, lines 1-51).

As per claim 21:

Wentker et al. and Muttik et al. substantially teach the apparatus described in claim 18. Wentker et al. further teach wherein said validation program is configured to evaluate third-party

software and attach a digital "valid" flag if the third-party software is found to be clean of known security compromising routines or attach a digital "invalid" flag to the third-party software if the third-party software is not found to be clean of known security compromising routines (col. 12, line 58 – col. 13, line 10 and col. 15, lines 1-19)

III. Claim 7 is rejected under 35 U.S.C. 103(a) as being unpatentable over Wentker et al., US Patent No. 6,481,632 and Muttik et al., US Patent No. 6,907,396, as applied to claim 1 above, and further in view of Brody, US Pub. No. 2001/0051928.

As per claim 7:

Wentker et al. and Muttik et al. substantially teach the method described in claim 1. Muttik et al. also teach a host computer (col. 3, lines 54-62). Furthermore, Muttik et al. teach that the computing environment allows for various computing systems, one of which may be a personal organizer (col. 3, lines 44-49). Not explicitly disclosed is wherein said method operates on a computer system which comprises a portable computing device coupled to said host computer and wherein the validating operation is performed by the host computer for the portable computing device. However, Brody teaches a PDA coupled to a host device for personalization purposes. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Wentker et al. to have the hand-held device coupled to the host computer in order to carry out different functions on the palmtop computing device. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Brody suggests that PDA's are used in conjunction with PC's in order to download

applications because PDA's are highly mobile and the client can always have access to his/her PDA in par. 33, lines 1-30.

IV. Claims 6, 14, and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wentker et al., US Patent No. 6,481,632 and Muttik et al., US Patent No. 6,907,396, as applied to claims 1, 8, & 18 above, and further in view of Ginter et al., US Patent No. 6,948,070.

As per claim 6:

Wentker et al. and Muttik et al. substantially teach the method described in claim 1. Not explicitly disclosed is wherein said validator program is specially constructed to reside in a secure fashion in the host facility of said computer system. However, Ginter et al. teach the use of a tamper-resistant security barrier which could be included in any component in a network so that processes are ensured to be carried out within a secure environment. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Wentker et al. for the validator program to be contained within a secure environment in order to ensure that it has not been tampered with so that it correctly validates the software/application. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Ginter et al. suggest that it is important to ensure that processes are carried out within a secure environment in col. 59, lines 48-59.

As per claim 14:

Wentker et al. and Muttik et al. substantially teach the apparatus described in claim 8. Not explicitly disclosed is wherein said validation program resides in said host computer of the computer system in a fashion intended to be secure. However, Ginter et al. teach the use of a

tamper-resistant security barrier which could be included in any component in a network so that processes are ensured to be carried out within a secure environment. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the apparatus disclosed in Wentker et al. for the validator program to be contained within a secure environment in order to ensure that it has not been tampered with so that it correctly validates the software/application. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Ginter et al. suggest that it is important to ensure that processes are carried out within a secure environment in col. 59, lines 48-59.

As per claim 19:

Wentker et al. and Muttik et al. substantially teach the apparatus described in claim 18. Not explicitly disclosed is wherein said validation program resides in said computer network in a fashion intended to be secure. However, Ginter et al. teach the use of a tamper-resistant security barrier which could be included in any component in a network so that processes are ensured to be carried out within a secure environment. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the apparatus disclosed in Wentker et al. for the validator program to be contained within a secure environment in order to ensure that it has not been tampered with so that it correctly validates the software/application. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Ginter et al. suggest that it is important to ensure that processes are carried out within a secure environment in col. 59, lines 48-59.

*References Cited, Not Used

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

1. US Patent No. 6,694,436
2. US Patent No. 5,953,502
3. US Patent No. 7,080,407
4. US Patent No. 6,981,279
5. US Patent No. 6,481,632 – cited in reference to an "open platform" architecture/system
6. US Patent No. 7,243,236
7. US Pub. No. 2002/0069263

The above references have been cited because they are relevant due to the manner in which the invention has been claimed.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nadia Khoshnoodi whose telephone number is (571) 272-3825. The examiner can normally be reached on M-F: 8:00-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

/Nadia Khoshnoodi/
Examiner, Art Unit 2437
2/1/2011

NK

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2437